UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/926,594	11/23/2001	You-Jin Eun	P21705	4083

7055 7590 08/10/2005

GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/926,594	EUN ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-33 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-33 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 23 November 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 3/8/02, 4/8/04.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-33 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1-33 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Regarding claims 1, 12 and 23, they recite the limitation "storing system security manager's certificate onto a security kernel when installing an operating system on a server computer". The disclosure teaches that the system security manager stores his/her certificate in the security kernel (Specification, p. 9, line 36 – p. 10, line 3); however, the disclosure fails to teach how such storing can be done when installing an operating system on a server computer. It is well known in the computer art that an operating system acts as an interface between a user of a computer and the computer hardware. Without an operating system having already been installed on the server computer, the user (i.e., the system security manager) would not be able to store data on the server. Thus, the disclosure fails to enable one skilled in the art to make and use

the claimed invention. Claims that are not specifically addressed are rejected by virtue of their dependency. For examination purpose, the limitation is interpreted as "storing system security manager's certificate onto a security kernel".

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 7-16, 18-27 and 29-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reardon (6,212,635) in view of Stein ("Web Security – A Step-by-Step Reference Guide").

Regarding claim 1, which is representative of claims 12 and 23, Reardon disclose a method for protecting a file system in a computer, wherein a user having an access authority for a file can access the file system in the computer (Abstract; col. 8, lines 26-29), the method comprising the steps of:

a) generating digital signature keys using security information of a system security manager and a corresponding certificate having the ID of the system security manager, the digital signature keys meets the limitation of system security manager's digital signature keys (col. 7, lines 56-60; col. 9, line 66 – col. 10, line 59);

b) storing the system security manager's digital signature keys in restricted memory of a security gateway which meets the limitation of a security kernel (col. 10, lines 56-59);

c) generating second digital signature keys and user's certificate (col. 11, lines 10-32);

d) setting an access authority of the file system (col. 11, lines 10-32);

e) identifying a user using a PIN when the user tries to access the file system (col. 11, lines 33-44); and

f) giving the user the access authority for the file in accordance with identification result (col. 11, lines 33-44).

Reardon discloses, in step b), storing the private key of the signature keys in the security kernel. Reardon does not disclose storing the private key together with the corresponding certificate. However, Examiner takes Official Notice that storing a private key together with the corresponding certificate is well known in the art. When a signature is generated using the private key, the corresponding certificate is sent together with the signature so that a receiving entity can use the public key from the accompanying certificate to verify the signature. It would have been obvious at the time of the invention was made to store the private key together with the corresponding certificate since storing a private key together with the corresponding certificate for ease of accessing the certificate is well known in the art. Accordingly, the certificate is stored in the security kernel.

Reardon discloses using a password based authentication method in step e). Reardon does not disclose using a signature based authentication method. Stein discloses using a signature based authentication method which is based on SSL (Secure Socket Layer) protocol (p. 292, Using Client Certificates for Access Control). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Reardon method to use a signature based authentication method, as taught by Stein, to overcome the vagaries of traditional password-based system.

Regarding claims 2, 13 and 24, Reardon further discloses the step of g) performing a user registering/deleting process if the user is identified as the system security manager (col. 11, lines 10-32; col. 15, lines 17-28).

Regarding claims 3, 14 and 25, Reardon further discloses the step of h) setting the access authority of the file system if the user is identified as the system security manager (col. 13, lines 8-37).

Regarding claims 4, 15 and 26, Reardon further discloses the step of i) accessing and processing a file (col. 11, lines 27-43).

Regarding claims 5, 16 and 27, Reardon further discloses that the digital signature keys generated in step a) comprises a public key and a private key (col. 10, lines 54-59).

Regarding claims 7, 18 and 29, Reardon further discloses providing the user with the file system access authority to the file system if the user is the general user and providing the user with registering/deleting authority, file system access setting authority and the file system access authority (col. 11, lines 10-43; col. 15, lines 17-28).

Regarding claims 8, 19 and 30, Reardon further discloses determining whether user registration or deletion is selected; deleting data related to a user to be deleted if the user deletion is selected; and registering a user if the user registration is selected; wherein the registering step includes providing the user to be registered with the access authority; generating a secret key and a public key of the user to be registered; generating a certificate of the user to be registered; encrypting and storing the secret key of the user to be registered; and storing the certificate of the user to be registered (col. 11, lines 10-32; col. 15, lines 17-28; col. 19, lines 8-16).

Regarding claims 9, 20 and 31, Reardon further discloses that the certificate is generated by encrypting the user's public key and the access authority (col. 6, lines 9-38; col. 15, lines 24-28; col. 18, line 54 – col. 19, line 1).

Regarding claims 10, 21 and 32, Reardon further discloses selecting a file; selecting a user allowed to be access the file; and setting the access authority to the file as an access authority of the user (col. 13, lines 8-37).

Regarding claims 11, 22 and 33, Reardon further discloses receiving a name of a file to be accessed; determining whether an access authority of the file to be accessed is equal to that of the system security manager; permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the system security manager; determining whether the access authority of the file to be accessed is equal to that of the user trying to access; and permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the user (col. 11, lines 33-43; col. 13, lines 8-37).

6. Claims 6, 17 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reardon in view of Stein as applied to claims 1, 12 and 23 above, and further in view of Abadi et al (5,315,657). As discussed in claim 1, Stein discloses using a signature based authentication method which is based on SSL (Secure Socket Layer) protocol. It is known in the art that the SSL (Secure Socket Layer) protocol authenticates a client by generating a random number at the server, sending the random number to the client, receiving the client's signature of the random number, verifying the client's certificate, extracting the client's public key from the certificate and verifying the signature to the random number. Reardon does not disclose that the manager is the certifying authority issuing the user's certificate (i.e., signing the user's public key). Abadi discloses that when a new user is added to a system, the system manager issues the new user's certificate which can be verified later using the system manager's public key (col. 7, lines 27-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Reardon and Stein such that the manager is the certifying authority issuing the user's certificate which can be verified later using the system manager's public key, as taught by Abadi. Certificates could be generated and issued more expeditiously with an in-house certifying authority.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,289,540 to Jones

Stallings, "Cryptography And Network Security – Principles And Practice"

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
8/4/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100